METHOD OF IMPLEMENTING THE DATA ENCRYPTION STANDARD WITH REDUCED COMPUTATION

ABSTRACT OF THE DISCLOSURE

An efficient software implementation of the round function of the Data Encryption Standard (DES) involves mathematical transformations performed on the DES round function and the DES round key computation function that reduce the computation required to complete a DES round on general-purpose, embedded, and cryptographic processors. These transformations shift computation associated with the Expansion Permutation from the DES round function to the DES round key computation function. As a result, fewer instructions are required to compute the inputs of the DES S-boxes in the round function.